

Equal sums of powers

Mathematics part II candidate D4171

Michaelmas and Hilary terms 1998–99

Contents

1	Introduction	3
1.1	Definitions	3
1.2	Euler’s Conjecture	4
2	Numerical records	4
2.1	Sums of two powers	4
2.2	Euler’s problem and variants	5
3	Implementation of the main searches	5
3.1	Sublists, secondary hashes and defeating $n \log n$	6
3.2	Getting hold of large amounts of CPU time	6
3.3	Looking for solutions to $\sum_{i=1}^4 x_i^5 = s^5$	7
3.4	Equal sums of three sixth powers	8
3.5	Results of the N_m^k computer searches	9
4	Some notes on elliptic curves	10
4.1	Weierstrass normal form	11
4.2	More advanced theorems about the structure of G_k	12
5	Elementary mathematical results	14
5.1	The obvious heuristics	14
5.2	$n_m^3(1)$ exists	14
5.3	Euler’s parametric solution to $x^3 + y^3 = z^3 + t^3$	16
5.4	Some notes on Euler’s problem	17
5.4.1	Bob Scher’s extra conditions for $k = 5$	17
5.4.2	Euler’s problem considered mod n	17
6	Parameterising $a^3 + b^3 = c^3 + d^3$ with quadratic forms	18
6.1	Methodology of the first computer search	19
6.2	Results of the computer search	20
6.3	Some less general but more productive forms	22
6.4	Looking for n -plets	24
6.4.1	A brute-force tactic which works	24
6.4.2	A more interesting tactic which doesn’t	24

7	Bounds on n_k^3	25
7.1	By elliptic curve addition	25
7.2	Some upper bounds – Hooley and Heath-Brown	26
8	Previous work on the fourth-power case	27
8.1	Euler’s parameterisation	27
8.2	Notes on the results of the exhaustive search, and Zajta’s paper .	28
9	Possible further work	29
A	Numbers writable in five ways as a sum of the cubes of two positive integers	31
B	Ramanujan-style solutions	32
B.1	General case, $ a , b , c \leq 20$	32
B.2	abb special case, $ a , b < 1200$	32
B.3	abc special case, $ a , b , c < 256$	33
C	Graphs	33

1 Introduction

1.1 Definitions

To begin at the beginning: let $U_k(x)$ be the number of ways that x may be written as a sum of two positive k th powers. This is probably most neatly explained in terms of generating functions : if we write

$$f_k(x) = \sum_{i=0}^{\infty} x^{r^k}$$

then

$$f_k(x)^2 = \sum_{i=0}^{\infty} U_k(i)x^i.$$

Where the equation $a^k + b^k = 2c^k$ is not solvable in non-trivial ($a \neq b$) positive integers, we have $U_k(i) = 1$ iff i is twice a k th power, and otherwise $U_k(i)$ is even (for, if i may be written as $a^k + b^k$ with $a < b$, it will also be counted as $b^k + a^k$). So we'll generally consider $u_k(i) = U_k(i)/2$.

Using Knuth's [7] notation for indicator functions, we define $N_m^k(n) = \sum_{i=1}^n (u_k(i) = m)$, the number of positive integers $\leq n$ which can be written in precisely m ways as a sum of two positive k th powers.

The asymptotics of N_m^k are, unfortunately, dominated by small known solutions; once it is known that

$$1729 = 1^3 + 12^3 = 9^3 + 10^3,$$

it is immediate that $N_2^3(x) \geq \frac{x^{1/3}}{1729}$ by considering things of the form $1729y^3$.

To remove this trivial lower bound and make the problem more interesting, therefore, we define $B_m^k(n)$ as the number of positive integers less than n which can be written as

$$x_1^k + y_1^k = x_2^k + y_2^k = \dots = x_m^k + y_m^k$$

where the x_i and y_i do not have a single shared common factor.

It turns out that, in the $k = 3$ case, there are techniques for constructing lots of rational solutions given a generating set; we get things of a shape like

$$425^3 + 753^3 = \frac{807^3 + 6361^3}{8^3} = \frac{6661^3 + 8315^3}{12^3} = \frac{435^3 + 1579^3}{2^3},$$

and multiplying a rational solution through by its common denominator gives a solution in integers with all the pairs of integers having a common factor. So we may want to make things harder for ourselves by defining $P_m^k(n)$ as the number of positive integers less than n , not divisible by any cube, and writable as a sum of two k th powers in precisely m ways.

At some points in the upcoming work, we will want to iterate over the numbers writable in a certain number of ways; therefore, we define $n_m^k(i)$ as the

least integer for which $N_m^k(n) = i$ – that is, we let (n_m^k) be a list of the integers writable in precisely m ways, with $n_m^k(1)$ the smallest number so expressible – and $p_m^k(i)$ and $b_m^k(i)$ similarly for P and B . Note that $b_m^k(1) = n_m^k(1)$, and that we have

$$N_m^k(x) \approx \sum_{i=1}^{B_m^k(x)} \left\lfloor \left(\frac{x}{b_m^k(i)} \right)^{1/3} \right\rfloor,$$

with the error term being due to elements of $n_M^k(x)$ with $M > m$.

1.2 Euler’s Conjecture

In 1769, Euler produced the related conjecture

Conjecture 1 (Euler’s Problem). *If $m < k$, there do not exist non-trivial sequences x_1, \dots, x_m with $\sum_{i=1}^m x_i^k$ a power of k*

For $k = 2$ there is clearly only the trivial solution; for $k = 3$ we have a simple case of Fermat’s last theorem, dealt with by Fermat; the proof is section 13.4 of Hardy and Wright ([10]). Wiles’ proof [23] of Fermat’s Last Theorem ensures us that we will must always have $m > 2$.

This is one of the few instances where Euler was wrong; in 1966 Lander [14] found a counterexample for $k = 5$ by computer search, and in 1988 Elkies [5] found a counterexample for $k = 4$ by using a parameterisation of the surface $r^4 + s^4 + t^2 = 1$ found by Demjanenko [2]; Frye later performed a computer search and found a counterexample with all the x_i less than 5×10^5 (given in section 2.2). No counterexample has been found yet for $k \geq 6$, though it is suspected that one will always exist.

2 Numerical records

2.1 Sums of two powers

1. $n_2^3 = 1729$ (Guy [8] says this is first mentioned by Bernard Frénicle de Bessy in 1657; it is the subject of a famous anecdote by Hardy)
2. $n_3^3 = 87539319$ (discovered by Leech [15] in 1956)
3. $n_4^3 = 6963472309248$ (discovered by Rosenstiel et al ([17]) in 1991)
4. $n_5^3 = 48988659276962496$ (my search – section 3)
5. $n_2^4 = 635318657$ (known to Euler, proved minimal by Leech [15])
6. $n_3^4 \geq 2^{80} \approx 1.2 \times 10^{24}$ (my search – section 3)
7. $n_2^5 \geq 2.4 \times 10^{22}$ (search by Randy Ekl [4])
8. $n_2^6 \geq 7.25 \times 10^{26}$ (search by Randy Ekl [4])

9. $p_2^3 = 1729$
10. $p_3^3 = 15170835645$ (Guy [8] notes this as discovered by Vojta in 1983)
11. $p_3^4 \geq 2^{60} \approx 1.15 \times 10^{18}$ (my search – section 3)

2.2 Euler’s problem and variants

1. The first solution discovered to $a^4 + b^4 + c^4 = d^4$ was

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

This is in Elkies [5], together with a proof that the rational points on $r^4 + s^4 + t^4 = 1$ are dense.

2. The smallest solution to $a^4 + b^4 + c^4 = d^4$ is

$$95800^4 + 217519^4 + 414560^4 = 422481^4;$$

the second-smallest solution has $d \geq 10^6$ (calculations by Frye, described in [5]).

3. $27^5 + 84^5 + 110^5 + 133^5 = 144^5$ was found by Lander [14], and there are no other primitive solutions to $\sum_{i=1}^4 x_i^5 = s^5$ for $s < 765$ [14], $s < 2834$ (a search performed by Sakellariou), or indeed $s < 32779$ (my search, section 3.3).
4. Bob Scher found that $14068^5 + 6237^5 + 5027^5 - 14132^5 - 220^5 = 0$ is the only solution of that form with largest entry less than 20000.
5. No solutions are known to $\sum_{i=1}^4 x_i^6 = \sum_{j=1}^2 y_j^6$, or to $\sum_{i=1}^5 x_i^6 = y^6$; there are 207 solutions to $\sum_{i=1}^3 x_i^6 = \sum_{j=1}^3 y_j^6$ with the GCD of the x_i and y_j both 1 and the common sum less than $5717^6 \approx 3.4 \times 10^{22}$ (another of my searches, section 3.4).

3 Implementation of the main searches

The searches for $n_m^k(1)$ and calculations of $N_m^k(x)$ can be considered as a matter of constructing very large tables of triples $(a, b, N = a^k + b^k)$, sorting to bring equal values of N together, and looking for equal N . Implementing them in this way is impractical, since we take $0 < a < b < 2^{20}$ and the full table would have 2^{39} entries.

The solution, of course, is to generate only sections of the table at a time. We pick a prime p , and construct, for each $m \in [0, p)$, the subset of the table with $N \equiv m \pmod{p}$, by running through $a = 0 \dots p$, computing $B = m - a^k \pmod{p}$, and adding $(a, b, a^k + b^k)$ to the table for all $b : b^k \equiv B \pmod{p}$ (using a precomputed table of k th roots modulo p).

We pick p just greater than 2^{20} , and the search limit is taken as p , so there is exactly one element below the search limit in each congruence class modulo p . Generally p is selected such that $x \rightarrow x^k$ is a bijection (for example, where $k = 3$ we insist on $p \equiv 5 \pmod{6}$); if this is impossible, as when k is even, we use a table containing -1 if b is not a k th-power residue and a pointer to a linked list of b 's k th roots otherwise.

It turns out that everything arranges itself nicely (that is, there are roughly the same number of entries in each congruence class), and, of course, the searches over different congruence classes are now independent so can be run on different computers.

3.1 Sublists, secondary hashes and defeating $n \log n$

It is a well-known result that sorting a list of n elements takes time $O(n \log n)$. However, we are here sorting only to collate, so we only require that identical values be sorted together; we can take advantage of this to get very close to $O(n)$.

Given any function ψ , we can split up the large array into many sublists, grouping together all the entries with the same value of $\psi(a^e + b^e)$; ψ is the *secondary hash*. In my case, because I'm using a binary computer, I use $\psi(a) = a \pmod{2^w}$ for some w ; I tried several different values of w , finding that $w = 19$ was best for this problem size on the sort of computers I used.

There is a mathematical justification for this choice of ψ ; p from the previous section is an odd prime, so we can use the Chinese Remainder Theorem to show that we're effectively replacing p with $2^w p$ and checking through 2^w congruence classes at a time.

Now, the sublists are quite short; everything remained nicely distributed, so the length had a mean of $2^{39}/2^{19}p \approx 1$. You can reject sublists with one entry at once, since they clearly can't contain a pair, and sorting short lists is extremely quick; the real advantage is that each sublist fits into the primary cache of the CPU, whilst sorting the complete list requires very many accesses to the (slow) main memory.

By this technique, we can get sorting time to take not much longer than generating the data, and the entire search takes about 1.5×10^6 seconds. This is feasible, but unpleasant, on a single computer. However, the search parallelises perfectly ...

3.2 Getting hold of large amounts of CPU time

I was able, by a series of e-mail and Usenet announcements, to get hold of 30 processors belonging to about 25 people (about a dozen Oxford undergraduates, and the rest spread all over the Western hemisphere) to run the search.

For the two-cubes search I used seven processors fairly efficiently for three days; for fourth powers, fifteen processors inefficiently for five days (fourth powers required multi-precision arithmetic, which made the search significantly slower than the cubic case), and for the search for $\sum_{i=1}^4 x_i^5 = y^5$ (in the next

subsection) I used perhaps sixteen processors efficiently for about a week, and about the same number again very inefficiently for nearly three weeks.

Much of this inefficiency was because I distributed the ranges and collected results manually by email, getting volunteers to run a benchmark program first to work out how large a range they should be given; for the fifth-powers search, I underestimated the number of volunteers I'd get, so the first ranges I handed out were far too large. Had I organised that search correctly, and had all the volunteers been available from the start, it would have been completed within three days.

I provided compiled versions of the search program for Linux and Windows, optimised for various Intel CPUs, and source code which was compiled on various Sparc and Alpha-based workstations. All the systems I used ran operating systems which supported pre-emptive multi-tasking, so the search ran in the background and the computers were still usable for non-compute-intensive operations while it ran. Some participants suspended the search when running memory-heavy programs such as *Netscape*, because otherwise the random accesses performed in a large memory array caused unacceptable swapping to disc.

The data was transferred to a central site (my desktop PC) by `ftp`, and analysed there by a variety of C programs.

3.3 Looking for solutions to $\sum_{i=1}^4 x_i^5 = s^5$

It is clearly impractical to check whether $a^5 + b^5 + c^5 + d^5$ is a fifth power for all $0 < a < b < c < d < N$, since the work involved would be $O(N^4)$. However, $O(N^2)$ storage is conceivable, so we can plan to check whether $a^5 + b^5 + c^5$ can be written in the form $e^5 - d^5$ ($e < d$).

And now we can split modulo p again. We note that $a^5 + b^5 + c^5 = e^5 - d^5$ only if the two sides are congruent modulo p , and pick p such that a search of size p^3 using memory p is conceivable (ensuring $p \not\equiv 1 \pmod{10}$ so that $x \rightarrow x^5$ is bijective and there is precisely one correct d for every e).

Now, run through $q = 0 \dots p - 1$. For each q , begin by listing the $\approx \frac{p}{2}$ solutions to $d^5 - e^5 \equiv q \pmod{p}$ with $e < d$, and adding the triple $(d, e, S = d^5 - e^5)$ to a table. Sort the table on S . Then run over the $\approx p^2$ solutions to $a^5 + b^5 + c^5 \equiv q \pmod{p}$, computing $a^5 + b^5 + c^5$ and looking for an entry in the first table with $S = a^5 + b^5 + c^5$. This last step is a binary search, which takes time $O(\log p)$, so the search complexity is $O(p^2 \log p)$ for each q , or $O(p^3 \log p)$ for the whole problem.

For p reasonably small, the Chinese Remainder Theorem permits us to perform the whole calculation using only 64-bit arithmetic : if we store the low 64 bits of $d^5 - e^5$ and compare with the low 64 bits of $a^5 + b^5 + c^5$, and remembering that our tables contain only numbers $\equiv q \pmod{p}$, we are effectively looking for simultaneous solutions modulo p and modulo 2^{64} – which translate by CRT to solutions modulo $2^{64}p$. Since the numbers involved are at most $3p^5$, we cannot get false positives provided we have $p < \sqrt[4]{2^{64}/3} = 49796$.

In fact, for speed, we use a variant on the sublist technique; we construct a table, indexed on the first 19 bits of the 64-bit entries, indicating the start and end of the range of entries with the first 19 bits matching. This lets us reduce the size of the search by a very large factor (or to skip the search altogether if the hash value doesn't appear), and a linear search over the very short section of table is then rather quicker than using the C library's binary search.

This technique can be modified to attack other problems; altering the list to contain also solutions to $d^5 + e^5 \equiv q \pmod{p}$ would roughly double the memory consumption, but *not* the run-time because of the use of binary search, and would let me find any solution to $\sum_{i=1}^5 x_i^5 = 0$. Unfortunately, I discovered that solutions of this form existed after I had already had to stop and restart the search twice because of subtle bugs in the program, so I couldn't face restarting the search a third time.

For exponent six, we could build a list of size p^2 containing things of the form $d^6 + e^6 - f^6$ to seek a counterexample to conjecture 1, or of the form $d^6 - e^6 - f^6$ to seek a solution to $\sum_{i=1}^4 x_i^6 = \sum_{j=1}^2 y_j^6$; because the inner loop is a binary search, the runtime would still be $O(p^3 \log p)$. I did not do this, but I used a slightly different technique to find equal sums of three sixth powers.

For conjecture 1 with exponent seven, we would again use a list of size p^2 , containing terms of the form $e^7 - f^7 - g^7$, but we would search over all quadruples $a^7 + b^7 + c^7 + d^7 : a^7 + b^7 + c^7 + d^7 \equiv m \pmod{p}$; this would take $O(p^4 \log p)$, which is perhaps too much on current computers. Possibly more likely to produce a result would be to fill the list with terms $e^7 + f^7 + g^7$ and search for $\sum_{i=1}^4 x_i^7 = \sum_{j=1}^3 y_j^7$ - the runtime would be the same.

3.4 Equal sums of three sixth powers

For three sixth powers, we can perform a very similar search to the ones for two cubes or two fourth powers; for $m = 0 \dots p - 1$, we store $(a, b, c, S = a^6 + b^6 + c^6 \pmod{2^{64}})$ for every $a, b, c : (a, b, c) = 1, 0 < a < b < c < p, a^6 + b^6 + c^6 \equiv m \pmod{p}$. Of course, we produce this by running over $0 < a < b < p$, and computing the permissible c using a precomputed array which contains -1 if a number had no sixth roots, or a pointer to a linked list containing its sixth roots if it had any; the modulo 2^{64} is implicit because we're using 64-bit arithmetic.

And, for $p < 5724$, we need only use 64-bit arithmetic; S will be less than $3p^6$, and (because we are restricting modulo p first) we can guarantee that two numbers will be reported equal iff they are equal modulo $2^{64}p$, which is greater than $3p^6$ within this range. 5717 is the largest prime less than 5724.

As always, we take the resulting arrays and sort to look for matches; since we require $a < b$ and further rule out a fairly large portion (≈ 0.723 experimentally) of the triples by requiring coprimality, the arrays are of size roughly $0.139p^2$ entries. For $p = 5717$, they fit in 90 megabytes of memory.

This memory use was considered unreasonable by most of my volunteers, so I added an option to write out the entries to four files on disc, choosing the file to use by looking at two middle bits of the sum and trusting to the operating system's buffering to avoid spending all the time seeking between blocks on disc,

and then to load these smaller files into memory and sorting; this was up to three times slower, but meant the program worked on computers with only 32 megabytes of available memory, and that the systems were more usable while the program ran.

Searching all 5717 congruence classes took about 1.2×10^{14} basic operations; inefficiently scheduled across four Pentium[-class systems, it took 50 hours, and found 207 numbers less than 3.4×10^{22} writable in two ways as a sum of three coprime sixth powers.

We never find both $\sum x_i^6 = \sum y_i^6$ and $\sum x_i^3 = \sum y_i^3$; however, only 22 of the solutions I obtained do *not* have $\sum x_i^2 = \sum y_i^2$. Guy [8] page 142 points out that Peter Montgomery had earlier found 18 such solutions.

We always have

$$\sum_{i=1}^3 x_i^6 = \sum_{j=1}^3 y_j^6 \implies \sum_{i=1}^3 x_i^2 - \sum_{j=1}^3 y_j^2 \equiv 0 \pmod{60}$$

since $u^6 - u^2 \equiv 0 \forall u \pmod{m}$ for $m = 3, 4, 5$, and hence by the Chinese Remainder Theorem we get equality modulo 60.

In fact, in all the solutions I've observed, the difference is divisible by 180, so is zero modulo 9, 4, 5. The result does not hold in general modulo 9 ($2^6 \equiv 4^6 \pmod{9}$) whilst $2^2 \equiv 4, 4^2 \equiv 7$), so there is probably something more complicated going on.

We observe differences of 51×180 and 55×180 , so there is no general congruence modulo anything larger than 180.

3.5 Results of the N_m^k computer searches

You have seen a very brief summary of the results in section 2. I have tried to put the more important features of the results into a series of graphs, which you will find in appendix C. The full numerical results are substantial (the list of n_2^3 is on the order of 300 megabytes); contact me if you want access to them.

All the graphs are plotted on log-log scales, so 'straight line' in the following means 'fitted well by $O(x^k)$ '

As you would expect from the discussion in the introduction, the N_k^3 graphs all tend to straight lines; rather more surprising is that the gradient of the straight lines does not appear to be the predicted $1/3$. Excel's curve-fitting algorithms (which are straightforward linear regression on $\log y$ against $\log x$), restricted to the portion of the graph with $N_k(x) \geq 50$ to avoid the rough distribution for x small whilst still incorporating as much of the data as possible, suggest that $N_2^3(x) = O(x^{0.45})$ and $N_k^3(x) = O(x^{0.40})$ for $k = 3, 4$.

There is a slight curvature to N_2^3 ; dividing out by powers of $\log x$ and fitting straight lines suggests that it could be explained by $N_2^3(x) = O(x^a(\log x)^b)$ for some $a \in (0.31, 0.38)$ and $b \in (2, 4)$. Using the same approach on N_3^3 gives an implausibly high power of $\log x$; this technique is probably doomed to failure due to lack of data to work from.

The B_k^3 graphs also seem to be tending to straight lines, but it is clearer that they are not all of the same gradient; Excel's curve-fitting algorithm suggests that $B_2^3 = O(x^{0.43})$ and $B_k^3(k > 3) = O(x^u)$ for $u < 0.3$. Again, dividing by powers of $\log x$ shows that a log term raised to a power between 1 and 4 would account for some of the curvature in B_2^3 .

The P_k^3 are also straight lines of clearly different gradient; P_2^3 has u rather greater than 0.4 and P_3^3 has u rather less than 0.3.

N_2^4 is fitted very well by $O(x^\gamma)$ with $\gamma \approx 0.26$; B_2^4 is fitted rather less well by $O(x^\gamma)$ with $\gamma \approx 0.14$. There is some slight curvature visible, but the technique of dividing by powers of $\log x$ does not work so well in this case; B_2^4 requires an implausibly high power, and N_2^4 is so well-fitted to start with that the improvements are invisible.

4 Some notes on elliptic curves

One of the easiest and most beautiful results in algebraic geometry is that the rational solutions to a cubic Diophantine equation have a group structure; this leads to a construction of new solutions from old ones, and is vital for most of the non-trivial bounds.

We consider the curve $x^3 + y^3 = k$ in projective 2-space ($\mathbb{R}^2 \cup \{\infty\}$, where parallel lines are defined to meet at infinity). The curve has a diagonal asymptote $x = -y$; we will say that ∞ thus lies on any line of gradient -1 .

Consider any two points (x_1, y_1) and (x_2, y_2) (neither equal to ∞ – we will handle that case separately) on the curve. Note first that there is a unique real $y = \sqrt[3]{k - x^3}$ with $x^3 + y^3 = k$, so we need only carry about the x coordinates of the points.

If $x_1 \neq x_2$, the two points define a line $y = mx + c$. If $x_1 = x_2$, we insist that the line be tangent to the curve at $x = x_1$; this gives us $m = -\frac{x_1^2}{y_1}$ by implicit differentiation, and then we can solve immediately for c . We run into a little trouble when $m = -1$; notice that this happens precisely if $x_1 = y_2$ and $y_1 = x_2$, or if one of the points is at ∞ .

Substituting the equation for the line into that for the curve $x^3 + y^3 = k$, we get

$$(1 + m^3)x^3 + 3cm^2x^2 + 3c^2mx + (k - c^3) = 0.$$

Now, this equation will certainly have the two real solutions x_1 and x_2 , and accordingly has a third real solution (for $m \neq -1$)

$$x_3 = \frac{k - c^3}{x_1x_2(1 + m^3)}, y_3 = mx_3 + c.$$

That is, the line will hit the curve at precisely one more point unless $m = -1$. Note that the coordinates of the new point are a *rational* function of those of the other two, so, if (x_1, y_1) and (x_2, y_2) had rational coordinates, so will (x_3, y_3) . If $m = -1$, let the third intersection be taken as ∞ .

So we define an operation $+$ on rational solutions by $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) = 0$, where $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ are colinear points of the curve. To convert this into a ‘friendly’ addition operation, we define negation as exchanging the x and y coordinates of a point (this makes sense since (x, y) is on the curve iff (y, x) is, and the line through (x, y) and (y, x) is parallel to the asymptote of the curve so meets it only at ∞); then $(x_1, y_1) + (x_2, y_2) = (y_3, x_3)$.

The operation has an identity element – the point at infinity (since, if (x, y) and ∞ lie on a line, the line has gradient -1 and passes through (y, x) ; reversing the coordinates as required gives $(x, y) + \infty = (x, y) -$ and an inverse (from the same construction, the inverse of (x, y) is (y, x)). It is clearly commutative. In fact, we have

Lemma 1. *The rational points of the curve $x^3 + y^3 = k$ form a group.*

We have a binary operation with an identity and an inverse; we need only prove it’s associative. The proof uses some slightly non-trivial projective geometry, and is somewhat tedious; see appendix A of [21] for the details.

Since, given x and y , we can compute $k = x^3 + y^3$ automatically, we can produce the function

$$(x, y) \rightarrow \left(\frac{y(2x^3 + y^3)}{y^3 - x^3}, \frac{x(x^3 + 2y^3)}{x^3 - y^3} \right)$$

for doubling a point.

Probably the neatest way of representing arithmetic on these curves is by a short *Maple* program:

```
xx:=a->a[1];
yy:=a->a[2];
ecdouble := a -> [(yy(a)*(2*xx(a)^3+yy(a)^3))/(yy(a)^3-xx(a)^3), \
  (xx(a)*(xx(a)^3+2*yy(a)^3))/(xx(a)^3-yy(a)^3)];
ecadd := proc(a,b) local m,c,front,const,ox,oy;
  if a=b then ecdouble(a,b);
  else
    m:=(yy(b)-yy(a))/(xx(b)-xx(a));
    c:=yy(a)-m*xx(a);
    const:=c^3-(xx(a)^3+yy(a)^3);
    ox:=-const/((1+m^3)*xx(a)*xx(b));
    oy:=m*ox+c;
    [oy,ox];
  fi;
end;
```

This represents points on the curve as two-member arrays; `ecadd` adds its arguments if they are different, and reduces to `ecdouble` if they are not.

4.1 Weierstrass normal form

In order to apply certain theorems, and to use pre-existing implementations of standard algorithms, we must put the curve $u^3 + v^3 = k$ into what is known as

Weierstrass normal form

$$y^2 = x^3 + ax + b.$$

This may be done (and it is a theorem that it may be done for any cubic curve) by a series of birational transformations. First, we put the curve into the projective form $u^3 + v^3 = kw^3$.

Substituting

$$\alpha = \frac{u+v}{2}, \beta = \frac{u-v}{2}, \gamma = w$$

converts the curve to $(\alpha + \beta)^3 + (\alpha - \beta)^3 = k\gamma^3$, or

$$2\alpha(\alpha^2 + 3\beta^2) = k\gamma^3.$$

We return to affine form by dividing through by α^3 , putting $\delta = \frac{\beta}{\alpha}$ and $\epsilon = \frac{\gamma}{\alpha}$, and getting

$$1 + 3\delta^2 = \frac{k}{2}\epsilon^3.$$

This is the right form - substitute $\zeta = 3\delta$ and multiply through by 3 to get $3 + \zeta^2 = \frac{3k}{2}\epsilon^3$; multiply through again by $144k^2$ to get $432k^2 + 144k^2\zeta^2 = 216k^3\epsilon^3$, write $\eta = 12k\zeta, \nu = 6k\epsilon$ to get $432k^2 + \eta^2 = \nu^3$, or

$$\eta^2 = \nu^3 - 432k^2. \tag{1}$$

For this result, see also exercise 1.13 of Silverman and Tate [21].

4.2 More advanced theorems about the structure of G_k

G_k is sometimes trivial - $x^3 + y^3 = 1$ has no rational solutions, by the $n = 3$ case of FLT, and so G_k consists only of the point at infinity. From the introduction to Knapp [13], we get that the Mordell-Weil theorem tells us that G_k is finitely generated - the number of generators of infinite order being called the *rank* r .

For dealing with sums of elements, it is sometimes useful to consider *heights*. The height of the rational a/b is defined as $H(a/b) = \max\{a, b\}$, and the height of the rational point $P = (x, y)$ on C as $H(x)$. Write $h(P) = \log H(P)$. It's clear that there can be only finitely many points on C of less than a given height - there are only finitely many **rationals** of less than a given height - and in addition we have (see for example Silverman [21] section III.1 lemmas 2 and 3) that

$$h(P + P_0) \leq 2h(P) + \kappa_0(C, P_0)$$

for some constant κ_0 depending on the curve and the starting point, and that

$$h(2P) \geq 4h(P) - \kappa(C)$$

for some κ dependent only on the curve.

For a curve C in Weierstrass normal form $y^2 = x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, we define the *discriminant* as the product

$$\Delta = ((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3))^2;$$

standard techniques of symmetric polynomials give us $\Delta = -4a^3 - 27b^2$. Define also the set T of exceptional primes as containing 2 and all the primes dividing the discriminant, and let $N_C(p)$ be the number of solutions to C considered as an equation over the field \mathbb{Z}_p , counting the point at infinity. In terms of Jacobi symbols,

$$N_C(p) = 1 + \sum_{x=0}^{p-1} 1 + \left(\frac{x^3 + ax + b}{p} \right).$$

Computing the rank in general is an open problem, and computing it rigorously in specific cases is often horrendously difficult. However, there is a wide-ranging conjecture (the Birch–Swinnerton-Dyer conjecture), one of whose simpler consequences suggests a numerical technique (Knapp’s [13] conjecture 1.9) – namely, that

$$\zeta(R) = \prod_{p \leq R, p \notin T} \frac{N_C(p)}{p} = O((\log R)^r).$$

I thought this was a promising technique for estimating r : compute $\zeta(R)$ for small primes, plot $\log \log R$ against $\log \zeta(R)$, and get r as the gradient of a best-fit straight line. Unfortunately, however, the partial products vary wildly (and extremely non-monotonically – the graphs look very like simulated Brownian motion) as we increase R , and it is impossible to fit a straight line to the results well enough to obtain a believable gradient. This is not too startling; Hasse’s Theorem states that

$$N_C(p) - p - 1 \in (-2\sqrt{p}, 2\sqrt{p}),$$

so the terms of the product are $1 + O(p^{-1/2})$ and get close to 1 only very slowly. I suspect the table in Knapp contains results from very carefully-contrived curves.

It is apparently rather easier to check whether a given set of points on a curve are independent – presumably by some technique providing effective estimates for the constants in the definition of the height, and then proving that any linear combination of the points must have a height greater than any of the points in the putative basis – thus providing a lower bound for the rank once we’ve found some integer points, but I was unable to find a reference to or an implementation of such techniques.

Unfortunately, no such simple theory as that for elliptic curves is available for higher powers or for more variables.

5 Elementary mathematical results

5.1 The obvious heuristics

We make the obviously false assumption that the k th powers of the positive integers less than N are uniformly distributed over $1 \dots N$ with $P(i = u^k : u \in \mathbb{N}) = N^{1/k}$, and the transparently insane one that, for $r < k$, the number of distinct sums of r k th powers in $1 \dots N$ is $O(N^{r/k})$. So far, this is not too stupid; Erdős and Mahler [6] produced in 1938 an elegant elementary proof (well-explained in Nathanson [16]) that the number of integers less than N writable as a sum of two positive integer cubes is $O(N^{2/3})$.

Now, we make the further ridiculous statement that the numbers of that form are uniformly distributed on $1 \dots N$, and in fact that $P(x \in [1, N] \text{ is a sum of } r \text{ } k\text{th powers}) = N^{-r/k}$. Assume these events are independent random variables, so the probability of being hit twice is the square of the probability of being hit once, and sum over $1 \dots N$ to get an estimate for the number of positive integers less than N writable in p ways as a sum of r positive k th powers:

$$N_{p,r}^k(x) \approx \begin{cases} O(\log x) & pr = k \\ O(x^{1-pr/k}) & pr \neq k \end{cases}.$$

We deduce that there ought to be solutions to $\sum_{i=1}^r x_i^k = \sum_{j=r+1}^k y_j^k$ for all j and k , but that (for example) $a^5 + b^5 = c^5 + d^5$ and $a^4 + b^4 = c^4 + d^4 = e^4 + f^4$ should have no solutions.

We can also use this technique to approximate P_n^k by the same expression, since P_n^k merely requires you to rule out all n divisible by a cube, and only a proportion $\zeta(3) - 1$ of n are such; we can absorb this constant factor into the O term.

We would also deduce that you can't write a number as a sum of two cubes in four or more ways; this is interesting given the result of the next subsection.

5.2 $n_m^3(1)$ exists

Hardy and Wright [10] give an elementary argument based on the two identities

$$X = \frac{x(x^3 + 2y^3)}{x^3 - y^3}, Y = \frac{y(2x^3 + y^3)}{x^3 - y^3} \implies X^3 - Y^3 = x^3 + y^3$$

and

$$x' = \frac{X(X^3 - 2Y^3)}{X^3 + Y^3}, y' = \frac{Y(2X^3 - Y^3)}{X^3 + Y^3} \implies x'^3 + y'^3 = X^3 - Y^3.$$

These are clearly variants on the algorithm for doubling a point on the elliptic curve, but with slightly altered signs so that the next part of the argument can assert that the result will be positive.

Expanding the double duplication, we get the staggeringly unhelpful expressions

$$f_1(x, y) = \frac{(x^{12} - 10x^9y^3 - 12x^6y^6 - 4x^3y^9 - 2y^{12})(x^3 + 2y^3)x}{(x^{12} + 14x^9y^3 + 24x^6y^6 + 14x^3y^9 + y^{12})(x^3 - y^3)}$$

and

$$f_2(x, y) = \frac{(2x^{12} + 4x^9y^3 + 12x^6y^6 + 10x^3y^9 - y^{12})(2x^3 + y^3)y}{(x^{12} + 14x^9y^3 + 24x^6y^6 + 14x^3y^9 + y^{12})(x^3 - y^3)}$$

with $f_1(x, y)^3 + f_2(x, y)^3 = x^3 + y^3$. We define $f(x, y) = (f_1(x, y), f_2(x, y))$.

We then pick a starting pair (x_1, y_1) , and repeatedly construct

$$(x_{i+1}, y_{i+1}) = f(x_i, y_i)$$

until we have enough (say n) terms. This is a sequence of pairs of rationals with $x_i^3 + y_i^3 = x_1^3 + y_1^3$; Hardy and Wright [10] notes that, if x is much greater than y , we have

$$\frac{f_1(x, y)}{f_2(x, y)} \approx \frac{x}{4y},$$

and therefore that, if we start with $(4^{n-1}, 1)$, all $n - 1$ of the derived rationals will be ≥ 0 .

Actually, if we start with $(3, 1)$, we have both coefficients positive for the first seven steps. To investigate this, define $s(n)$ as the least x such that $f^i(x, 1)$ has both coefficients positive for $i = 0..n$ and at least one negative for $i = n + 1$.

A quick search written in C++ (with the results checked using *Maple's* 100-digit arithmetic) gave the results in the table below and in the graph 'Minimum start values for given persistence' in appendix C. Excel's curve-fitting suggests that $s(n) \approx 1.65^n$.

n	$s(n)$	n	$s(n)$
7	3	24	182796
9	145	26	186027
11	179	27	733874
13	181	29	742109
14	724	30	2935465
15	2353	31	2976603
16	9412	32	2976617
17	11459	33	9639687
18	11582	34	11906414
21	12175	36	38552058
23	45699	37	50647985

We then take our sequence of positive rationals, and multiply through by the common denominator. As you can see, the denominators of x_i and y_i are

equal; if x_1 and y_1 were integers, the common denominator of $x_1 \dots x_n$ is that of x_n .

The numerator and denominator of x_i are of order $x_1^{15^i}$, whilst (clearly) $x_i \in (0, \sqrt[3]{x_1^3 + y_1^3})$; accordingly, we get a solution with the sum $S_n = x_n^3 + y_n^3$ being of the order $x_1^{3 \times 15^i}$. For an explicit example, we start with $(x_1, y_1) = (3, 1)$, so $S_1 = 28$. We find that $S_2 \approx 10^{24}$, $S_3 \approx 10^{376}$, $S_4 \approx 10^{6009}$, and that S_5 has 73790 digits.

5.3 Euler's parametric solution to $x^3 + y^3 = z^3 + t^3$

Both Hardy and Wright [10] and Dickson [3] give a parameterisation due to Euler of the solutions to the above equation in rationals of either sign. We reparameterise as $x = a + b, y = a - b, z = c + d, t = c - d$, turning the equation into $a(a^2 + 3b^2) = c(c^2 + 3d^2)$. Working over the UFD $\mathbb{Q}(\sqrt{-3})$, we get

$$a(a - b\sqrt{-3})(a + b\sqrt{-3}) = c(c - d\sqrt{-3})(c + d\sqrt{-3}).$$

Define u and v by

$$\frac{c + d\sqrt{-3}}{a + b\sqrt{-3}} = u + v\sqrt{-3}.$$

Then we have $c = ua - 3vb, d = va + ub$, and considering norms we get $a = c(u^2 + 3v^2)$. Comparing the two expressions for c , we get a linear relation

$$(u(u^2 + 3v^2) - 1)a = 3v(u^2 + 3v^2)b.$$

Write $\alpha = u(u^2 + 3v^2) - 1, \beta = 3v(u^2 + 3v^2)$; provided α and β are not both zero (in which case $u = 1, v = 0, c = a, d = b$, and $x = z, y = t$ and the solution is uninteresting), we have $\alpha a = \beta b$, so can divide through by $\alpha\beta$ to define $w = a/\beta = b/\alpha$. Now we can substitute back for c and d and thence for x and y . We get

$$\begin{aligned} x &= w(1 - (u - 3v)(u^2 + 3v^2)) \\ y &= w((u + 3v)(u^2 + 3v^2) - 1) \\ z &= w((u + 3v) - (u^2 + 3v^2)^2) \\ t &= w((u^2 + 3v^2)^2 + (3v - u)) \end{aligned}$$

Clearly integral values of u and v give integral solutions, and if we are distrustful of solutions with a common factor we must have $w = \pm 1$. The argument we used shows that any quadruple (x, y, z, t) satisfying $x^3 + y^3 = z^3 + t^3$ satisfies Euler's form, and in particular that any given solution will be produced by precisely one set of coefficients.

Unfortunately, z is almost always negative, so we usually need to take w negative; more unfortunately, solutions in positive integers to the original equation tend to lead to u, v, w as inconvenient rationals of varying signs.

5.4 Some notes on Euler's problem

5.4.1 Bob Scher's extra conditions for $k = 5$

In 1992, Bob Scher discovered a straightforward theorem which made exhaustive search for solutions to $\sum_{i=1}^5 x_i^5 = 0$ rather quicker [18]; I found out about these after performing my search. In conjunction with Ed Siedl, then at Sandia National Laboratories, implemented a search on a 72-node Paragon supercomputer and discovered

$$14068^5 + 6237^5 + 5027^5 - 14132^5 - 220^5 = 0$$

The relevant theorem is

Theorem 1. *If $\sum_{i=1}^5 a_i^5 = 0$, with $\gcd(a_1, a_2, a_3, a_4, a_5) = 1$, then there are either one or two pairs of a_i which sum to zero modulo 5.*

Proof. We work modulo 25, noting that $0^5 \equiv 0$, $1^5 \equiv 1$, $2^5 \equiv 7$, $3^5 \equiv -7$, $4^5 \equiv -1$ – that is, that the non-zero values appearing are ± 1 and ± 7 . Since $\sum a_i^5 = 0$, we have $\sum a_i^5 \equiv 0 \pmod{25}$. But $7i + j = 25z$ has no solutions over the integers with $|i| + |j| \leq 5$, so we can't have a non-obvious cancellation. So we must have a occurrences of 0, b occurrences of 1 and -1 , and c occurrences of 7 and -7 , with $a + 2b + 2c = 5$ and $a, b, c \geq 0$; we can't have $a = 5$ because of the gcd condition, so the solution must look like the one in the theorem. \square

5.4.2 Euler's problem considered mod n

Modulo n , Euler's problem will always have solutions (if only $0^k + \dots + 0^k = 0^k$); let $u_n^k(i, m)$ be the number of ways i can be written as the sum of n k th powers modulo m .

In general, the function $\psi_n(m) = u_n^n(0, m)$ will be multiplicative, by the Chinese Remainder Theorem, so we have to consider $\psi_n(p^k)$. We can compute ψ_n quickly by noting that

$$u_n^k(i, m) = \sum_{j=0}^m u_{n-1}^k(i - j^k, m),$$

so we compute $u_1^k(i, m)$ for all $i \pmod{m}$ by constructing an array of counters and then running through the i incrementing counter number i^k .

We then compute $u_2^k(i, m)$ for all i using the sum above, and carry on computing $u_{r+1}^k(i, m)$ using the table of results for u_r^k until we have reached the desired point. This takes about $m^2/4$ microseconds for $n = 5$ on a home PC.

Theorem 2. *For q prime,*

$$\psi_q(p) = p^{q-1} \quad \text{whenever } p \not\equiv 1 \pmod{q}$$

Proof. If $p \not\equiv 1 \pmod{q}$, then the order of \mathbb{Z}_p is not divisible by q . Since q is prime, this means there are no elements of order divisible by q , and so $x \rightarrow x^q$

is a bijection (since $u^q = v^q \implies (uv^{-1})^q = 1$). In that case, any $q - 1$ -plet of elements of \mathbb{Z}_p may be extended in precisely one way to an q -plet by letting

$$x_q = \left(\sum_{i=1}^{q-1} x_i^q \right)^{-q}.$$

□

$\psi_n(p)$ generally increases with p , though this is not a theorem; there are many counterexamples with $n = 3$, and $\psi_5(193) < \psi_5(191)$. When $p \equiv 1 \pmod{n}$, $\psi_n(p)$ appears to be $p^{n-1} + O(p^{n-2})$, with the constant in the O notation having $|k| < 8$ for $p < 10^4$.

It appears that $\psi_n(p) \equiv 1 \pmod{n}$ for $p \neq n$; surprisingly, it also seems that $\psi_n(p) \equiv 1 \pmod{10}$ and $\psi_n \in \{1, 21, 41, 51, 61, 81\} \pmod{100}$.

6 Parameterising $a^3 + b^3 = c^3 + d^3$ with quadratic forms

In [11], Hooley makes use of the identity

$$(4x^2 - 4xy + 6y^2)^3 + (3x^2 + 5xy - 5y^2)^3 = (6x^2 - 4xy + 4y^2)^3 + (-5x^2 + 5xy + 3y^2)^3$$

due to Ramanujan to provide a lower bound of the form $O(x^{1/3} \log x)$ for $\sum_{i=1}^x (u_3(x) > 1)$. Dickson [3] offers another solution,

$$(7x^2 - 16xy - 3y^2)^3 + (14x^2 + 4xy + 6y^2)^3 = (14x^2 - 4xy + 6y^2)^3 + (7x^2 + 16xy - 3y^2)^3$$

found by Gérardin in 1912. I was rather surprised by the existence of two such simple partial parameterisations, and so conducted a search for others.

In this section, I will write the quadratic form $ax^2 + bxy + cy^2$ as $f_{a,b,c}$, and call solutions parameterised by quadratic forms *Ramanujan-class*.

As an aside, the Ramanujan-class solutions may be interpreted as confining the results to a plane in projective space. We have four quadratic forms $p = f_{a,b,c}(x, y)$, $q = f_{d,e,f}(x, y)$, $r = f_{a',b',c'}(x, y)$, $s = f_{d',e',f'}(x, y)$ with $p^3 + q^3 = r^3 + s^3$.

Note that (a, b, c) , (d, e, f) , (a', b', c') , (d', e', f') are four three-element vectors over \mathbb{Q} , and hence that there exists some combination

$$\alpha(a, b, c) + \beta(d, e, f) + \gamma(a', b', c') + \delta(d', e', f')$$

which is everywhere zero. Now, note that

$$f_{a,b,c} = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \cdot \begin{pmatrix} x^2 \\ xy \\ y^2 \end{pmatrix},$$

so

$$\alpha p + \beta q + \gamma r + \delta s = \begin{pmatrix} x^2(\alpha a + \beta d + \gamma a' + \delta d') \\ xy(\alpha b + \beta e + \gamma b' + \delta e') \\ y^2(\alpha c + \beta f + \gamma c' + \delta f') \end{pmatrix} = \mathbf{0}.$$

So the solutions generated by this form lie on the plane $\alpha r + \beta s + \gamma t + \delta u = 0$ in projective 3-space, and also on the surface $S : r^3 + s^3 - t^3 - u^3 = 0$; these intersect in a cubic curve. The fact that this cubic curve of intersection can be parameterised with quadratic forms rather than elliptic functions indicates that it is singular; this observation could probably be used to produce a more efficient search by constructing planes deliberately tangent to S .

6.1 Methodology of the first computer search

The idea is to look for equal sums of the cubes of two quadratic forms, by running over all values of the six defining coefficients in $f_{a_1, a_2, a_3}^3 + f_{b_1, b_2, b_3}^3$ within a convenient range, evaluating the quadratic forms, storing the result in a list and sorting it.

The obvious approach would be to expand this into a homogenous polynomial of degree six, and carry around the seven integer coefficients of $x^i y^{6-i}$. However, this would take up lots of storage and be rather cumbersome to manipulate.

Instead, I noted that a quadratic form is in general defined by its value at three fixed points, since we can solve the three simultaneous equations

$$ax_i^2 + bx_i y_i + cy_i^2 = v(x_i, y_i) \quad i = 1 \dots 3$$

provided that we haven't made a pathological choice of the x_i and y_i which makes the determinant of the relevant matrix zero, and accordingly that it's defined by the cube of its value at three fixed points (since cubing is bijective).

This would mean I needed only carry around three integers per form, but this is still fairly cumbersome.

So I considered the function

$$K(a, b, c) = f_{a,b,c}(1, 2)^3 + 3.14159f_{a,b,c}(3, 5)^3 + 2.71828f_{a,b,c}(7, 11)^3 \quad (2)$$

mapping quadratic forms $ax^2 + bxy + cy^2$ to elements of \mathbb{R} . Clearly

$$K(a, b, c) + K(d, e, f) = K(a', b', c') + K(d', e', f') \quad (3)$$

is a necessary condition for

$$f_{a,b,c}^3 + f_{d,e,f}^3 = f_{a',b',c'}^3 + f_{d',e',f'}^3 \quad (4)$$

and K is a sufficiently complicated and unnatural object that I hoped there would be few coincidences.

I began by constructing the obvious enumeration $f_0 \dots f_{(2k+1)^3-1}$ of the quadratic forms $f_{a,b,c}$ with $|a|, |b|, |c| \leq k$, by labelling $f_{a,b,c}$ as $(2k+1)^2 \times (a+k) + (2k+1) \times (b+k) + (c+k)$; let $a(i), b(i), c(i)$ be the functions to get a, b and c given this numbering.

I then labelled each form with the value $\kappa(i) = K(a(i), b(i), c(i))$, and constructed the set of pairs $(x, y) : 0 \leq x \leq y \leq (2k+1)^3 - 1$, labelling each with the

real number $\kappa(x)+\kappa(y)$, before sorting the set by label (rejecting pairs with label 0, since these tended to correspond to identities of the form $f_i - f_i = f_j - f_j$).

I ran through the sorted set, taking every pair (x, y) and (z, t) with labels differing by less than 0.01 (because floating-point arithmetic is inherently imprecise), converting back to quadratic forms, and checking that the coefficients of $x^i y^{6-i}$ in equation 4 were all zero to rule out coincidences where equation 3 holds but 4 does not. If they were, I displayed the twelve coefficients.

The implementation is not completely straightforward, since 12 bytes are required to store the pair number and the label, and there are (for $k = 21$, which was the largest search I did) rather over 3 billion pairs. It was not obviously possible to use congruence methods, so instead I constructed and sorted the set once for each value of $i \in [0, 511]$, each time throwing out pairs with the middle 9 bits of the internal representation of the floating-point label not equal to i . This increased the runtime by a factor 512, but reduced memory usage by the same factor so the search fitted in 100 megabytes. It took a couple of days to run on a single fast desktop PC.

6.2 Results of the computer search

Most of the results were extremely unexciting statements of the form $(af)^3 + (bf)^3 = (cf)^3 + (df)^3$ for some form f and some quadruple

$$(a, b, c, d) : a^3 + b^3 = c^3 + d^3;$$

since we're allowing negative entries now, we get things like $3^3 + 4^3 + 5^3 = 6^3$ as well as $1^3 + 12^3 = 9^3 + 10^3$. We weed these out by dividing through by the GCD and then comparing against a pre-generated table.

Also, the search technique does not take account of the many symmetries of the equations – we can rearrange the components on both sides, and swap x and y in the quadratic forms – so each identity occurred many times in the final list.

This duplication is weeded out by defining a *normal form* for such an identity; begin by removing any common factor shared by all 12 coefficients. Then define a weight function

$$w(f_{a,b,c}) = a^2 + b^2 + c^2,$$

and sort the components of the identity (with appropriate change of signs) such that it ends up as $f_1^3 + f_2^3 = f_3^3 + f_4^3$ with $w(f_1) \leq \dots \leq w(f_4)$; break ties by lexicographical ordering on the absolute values of the coefficients.

Inspecting a list which had been put into this preliminary normal form let me notice

Theorem 3. *If*

$$f_{a,b,c}^3 + f_{d,e,f}^3 = f_{a',b',c'}^3 + f_{d',e',f'}^3$$

then

$$f_{a,-b,c}^3 + f_{d,-e,f}^3 = f_{a',-b',c'}^3 + f_{d',-e',f'}^3.$$

Proof. We expand equation 4 to get

$$\begin{aligned}
& (a^3 + d^3)x^6 + \\
& (3a^2b + 3d^2e)x^5y + \\
& (3a(b^2 + ac) + 3d(e^2 + df))x^4y^2 + \\
& (b(b^2 + 6ac) + e(e^2 + 6df))x^3y^3 + \\
& (3c(b^2 + ac) + 3f(e^2 + df))x^2y^4 + \\
& (3bc^2 + 3ef^2)xy^5 + \\
& (c^3 + f^3)y^6
\end{aligned} \tag{5}$$

and notice that b and e always appear either squared (and hence unaffected by negation) or multiplying some other expression such that the value will merely be negated on replacing $b \rightarrow -b$, $e \rightarrow -e$. So such a negation merely negates the coefficients of $x^{2k+1}y^{5-2k}$, and applying the negation to both sides keeps the equality intact. \square

With this ordering established, we can define a_i, b_i, c_i by $f_i = f_{a_i, b_i, c_i}$. We insist that $a_1 \geq 0$, negating the whole expression if this is false, and that $b_j > 0$ where j is minimal with $b_j \neq 0$, negating all the b_i if that is false.

The roles of a and c in equation 5 are symmetric, so we can further ensure that, for i minimum with $|a_i| \neq |c_i|$, $|c_i| > |a_i|$ (by swapping all the a and c if this is false).

In one case this did not give a unique form for an expression, so we add the ad-hoc rule that, once all these procedures have been carried out, we ensure that, if $|a_3| = |a_4|$, then $a_4 < a_3$ (to put the positive term as far forward as possible).

For example, the normal form of Ramanujan's inequality is

$$f_{3,-5,-5} + f_{5,5,-3} = f_{-4,-4,-6} + f_{6,4,4}.$$

We get 20 non-trivial solutions, with Ramanujan's being the one of least sum-of-weights; the list appears in appendix B.1.

Quadratic forms come in three sorts – positive definite which can never take values < 0 , negative definite which can never take values > 0 , and agnostic (or more prosaically indefinite) which can take any values. At first the presence of the latter two classes seems an insuperable obstacle to producing large numbers of solutions in positive integers, but it appears that often you can rearrange $a + b = c + d$ such that negative-definite terms are paired with agnostics, and then find a region of values for x and y in which everything is positive.

6.3 Some less general but more productive forms

In the output of the previous search, I noted the existence of Ramanujan's identity and of the similar-shaped one

$$(7, -17, -17) + (14, 20, 20) = (20, 20, 14) + (-17, -17, 7),$$

so wondered whether there might be a pattern of things of this sort. Rearranging into the shape

$$(7, -17, -17) + (17, 17, -7) = (20, 20, 14) + (-14, -20, -20),$$

it becomes clear that we want to find values of a, b such that $u_{a,b}(x, y) = u_{c,d}(x, y)$, where

$$u_{a,b}(x, y) = (ax^2 + bxy + by^2)^3 - (bx^2 + bxy + ay^2)^3.$$

Expanding $u_{a,b}(x, y)$ gives us

$$u_{a,b}(x, y) = (a^3 - b^3)(x^6 - y^6) + 3xyb(a^2 - b^2)(x^4 - y^4 + xy(x^2 - y^2)) \quad (6)$$

so I wrote a search routine to look for values of (a, b) and (c, d) with $a^3 - b^3 = c^3 - d^3$ and $a^2 - b^2 = c^2 - d^2$.

This required only k^2 rather than k^6 storage, so I was able to search over $0 < |x|, |y| < 1200$; to my slight surprise, I found 27 solutions, listed in appendix B.2. I call things of this sort *abb* solutions; they correspond to solutions with $p + q = k(r + s)$ for $k = \frac{a+b}{c+d}$ and p, q, r, s as in the aside in section 6, and it appears that the values produced by one *abb* solution will never be repeated in a second one.

A later look at the table of results from the large test suggested that the shapes

$$(a, b, c) + (-a, b, -c) = (d, e, f) + (-d, e, -f)$$

and

$$(a, b, c) + (-c, -b, -a) = (d, e, f) + (-f, -e, -d)$$

might also be fruitful. So we define

$$v_{a,b,c}(x, y) = (ax^2 + bxy + cy^2)^3 - (ax^2 - bxy + cy^2)^3$$

and

$$w_{a,b,c}(x, y) = (ax^2 + bxy + cy^2)^3 - (cx^2 + bxy + ay^2)^3,$$

and expand as before to get

$$v_{a,b,c}(x, y) = 6bc^2xy^5 + 2b(b^2 + 6ac)x^3y^3 + 6a^2bx^5y \quad (7)$$

$$w_{a,b,c}(x,y) = (a^3 - c^3)(x^6 - y^6) + 3b(a^2 - c^2)xy(x^4 - y^4) + 3(a-c)(b^2 + ac)x^2y^2(x^2 - y^2) \quad (8)$$

So $v_{a,b,c} = v_{a',b',c'}$ requires

$$\begin{aligned} bc^2 &= b'c'^2 \\ b(b^2 + 6ac) &= b'(b'^2 + 6a'c') \\ a^2b &= a'^2b' \end{aligned} \quad (9)$$

The value of equation 7 is unaffected by negating b or by negating both of a and c , and is zero if $b = 0$, so I ran a search with $a \in [0, 256]$, $b \in [1, 256]$, $c \in [-200, 256]$ which gave several primitive solutions, each repeated twice because $v_{a,b,c} = v_{d,e,f} \implies v_{c,b,a} = v_{f,e,d}$; I removed them by a primitive variation on the normal form technique – constructing norms $a^2 + b^2 + c^2$ and $d^2 + e^2 + f^2$ next to each solution, swapping the sides round so the norms were in increasing order, and then sorting by norm.

The most obvious observation from the first table of solutions was that $v_{a,b,c} = v_{d,e,f} \implies v_{a,bu,cu^2} = v_{d,euf,fu^2}$ – expanding out shows that the powers of u happen to coincide precisely with the powers of y , so this is a theorem. Weeding out such solutions is not entirely straightforward – the factors are hidden by the removal of common factors earlier – but gives the rather short list

$$\begin{aligned} v_{6,4,14} &= v_{3,16,-7} \\ v_{21,81,-26} &= v_{63,9,78} \\ v_{31,125,-42} &= v_{155,5,210} \\ v_{35,128,-39} &= v_{140,8,156} \end{aligned}$$

of primitive solutions in this range; I'm not entirely convinced the second and fourth are different.

Similarly, $w_{a,b,c} = w_{a',b',c'}$ needs

$$\begin{aligned} a^3 - c^3 &= a'^3 - c'^3, \\ b(a^2 - c^2) &= b'(a'^2 - c'^2), \\ (a-c)(b^2 + ac) &= (a'-c')(b'^2 + a'c') \end{aligned} \quad (10)$$

The value of equation 8 is zero for $a = c$, and unaffected by negating b , so we can restrict to $a \neq c, b > 0$. It is also unaffected by swapping a and c and then negating both, but this was rather harder to code for. So I searched for $a \in [-256, 256]$, $b \in [1, 256]$, $c \in [-256, 256]$ (using the slicing technique of section 6.1 to reduce memory requirements), and removed duplicates using normal forms; most solutions appeared four times, because $w_{a,b,c} = w_{d,e,f} \implies w_{-a,b,-c} = w_{-d,e,-f}$, $w_{c,b,a} = w_{f,e,d}$ and $w_{-c,b,-a} = w_{-f,e,-d}$. This list is longer, and appears in appendix B.3.

6.4 Looking for n -plets

6.4.1 A brute-force tactic which works

We now have a technique for generating a fairly large number of numbers writable as the sum of two integer cubes (not necessarily positive) in two ways. So, we can construct a large table of $(a, b, c, d, S = a^3 + b^3)$ with $a^3 + b^3 = c^3 + d^3 = S$, and then use similar techniques to the main search to find coincident S in this.

The method used takes a Ramanujan set (a quadruplet of quadratic forms) as a parameter, and runs over $x, y : 0 < x < 100, -100 < y < 100$ (since $f(x, y) = f(-x, -y)$ because quadratic forms are homogenous), evaluating the forms at each point to produce a quadruple of integers (a, b, c, d) with $a^3 + b^3 = c^3 + d^3$. If possible, it rearranges and changes signs to convert the quadruple to one with $a < b, c < d, a < c, a, b, c, d > 0$; if this is not possible the quadruple is discarded.

When fed with a large collection of the abb parameterisations, this technique gave no results at all; when fed with even a small subset of the ‘random-looking’ results produced by the main search, quite a promising number of triples were discovered.

After having a look at the form of the known quadruplets, I modified the program slightly so that, instead of outputting (a, b, c, d) , it removed common factors to get (a', b', c', d') ; I then sorted the output list to remove duplicates, ran a script which read (a', b', c', d', S) and outputted $(ka', kb', kc', kd', k^3S)$ for $1 \leq k \leq 12$, sorted again to remove duplicates and combined by values of S ; this produced a few more triplets, though no quadruplets.

6.4.2 A more interesting tactic which doesn't

A mathematically more interesting way of finding triplets would be to look for quadratic-form parameterisations $\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2$ and $\mathbf{x}_1, \mathbf{x}_2, \mathbf{z}_1, \mathbf{z}_2$ in which both entries on one side are equal, which will produce parametric solutions for triplets. There are four such in appendix B :

$$\begin{aligned}
 f_{3,-5,-5}^3 + f_{-6,-4,-4}^3 &= f_{3,11,3}^3 + f_{-6,-8,-6}^3 \\
 &= f_{-5,-5,3}^3 + f_{-4,-4,-6}^3 \\
 f_{3,-1,-7}^3 + f_{-6,16,-14}^3 &= f_{-5,15,-7}^3 + f_{-4,12,-14}^3 \\
 &= f_{3,-17,17}^3 + f_{-6,20,-20}^3 \\
 f_{6,3,9}^3 + f_{8,17,-1}^3 &= f_{9,15,12}^3 + f_{-1,-19,-10}^3 \\
 &= f_{12,9,6}^3 + f_{-10,-1,8}^3 \\
 f_{6,4,14}^3 + f_{-3,-16,7}^3 &= f_{5,0,-17}^3 + f_{4,0,20}^3 \\
 &= f_{6,-4,14}^3 + f_{-3,16,7}^3
 \end{aligned}$$

However, whilst it's trivially possible to convert anything of the form $a - b = c - d$ into a solution in positive integers, you can't do something similar with $a + b = c + d = e + f$; anything which corrects two of the terms must have entries from both those terms and not the third, and so will give something not a sum of two terms only when applied to the third term. And none of these triplets seems ever to have all terms positive (certainly not for $x, y \in [-1000, 1000]$), so we do not have a parametric triplet solution yet.

7 Bounds on n_k^3

The bound we get from the technique of Hardy and Wright is that

$$\log n_k^3(1) \approx O(k \times 15^k).$$

The results of the computer search, however, suggest that $n_k^3(1)$ is reasonably well-approximated by $0.53 \times 17000^{k-1}$ – and in particular that its behaviour is not drastically double-exponential. So we want a better bound.

7.1 By elliptic curve addition

The major difficulty with looking for new solutions by elliptic curve operations is that elliptic curves stretch off to infinity in both directions, and accordingly that not all the points will have both co-ordinates positive.

In fact, divide the curve $x^3 + y^3 = K$ into three portions: C_1 with negative x and positive y coordinate, C_2 with both coordinates positive, and C_3 with positive x and negative y . Now C_1 and C_3 are both strictly concave, whilst C_2 is strictly convex; we may deduce that a sum of two points in the same portion cannot lie in that portion.

We therefore become compelled to use something like Hardy and Wright's construction, and this gives an enormous lower bound because we are generating a point of order k through k quadruplings, each of which raises the common denominator to the fifteenth power, and then multiplying through by the cube of that common denominator.

By trial, neither $b_5^3(1)$ nor $b_5^3(2)$ can be extended to a solution with six terms by multiplying by $m \leq 13$ and searching for another point on the curve; also, a search over all sums of fairly small (≤ 6) numbers of known points on the curves revealed nothing with a denominator less than 10^7 .

In the hope of finding reasonable upper bounds for $b_k^3(k = 6, 7, 8)$, I wrote a *Maple* program to consider the curves corresponding to all 154 values of $b_4^3(j)$ that I'd found. Let $P_1(j), \dots, P_4(j)$ be the four positive-integer points on $x^3 + y^3 = b_4^3(j)$.

For each j , I ran over all ordered quadruples from $\{P_1(j), \dots, P_4(j)\}$, computing the sum; running over unordered quadruples would have been more efficient but harder to program, and the extra efficiency was unnecessary since the task completed in a few minutes anyway. If the sum (x, y) had $x > 0, y > 0$,

and was not one of the known positive integer points, I stored the common denominator of x and y in a list L .

Once all the quadruples had been examined, I sorted L , and labelled the curve with the LCM of its two smallest elements, before proceeding to the next curve.

Once all the curves were done, I sorted them by label. The smallest label was 201, attached to $x^3 + y^3 = 1013538931200793088$, and giving $b_6^3(1) < 8.2 \times 10^{24}$ – specifically,

$$\begin{aligned}
8230545258248091551205888 &= 159363450^3 + 161127942^3 \\
&= 125436328^3 + 184269296^3 \\
&= 85970916^3 + 196567548^3 \\
&= 63273192^3 + 199810080^3 \\
&= 17781264^3 + 201857064^3 \\
&= 11239317^3 + 201891435^3
\end{aligned}$$

Modifying the program to consider the LCM of the three or four smallest denominators gave estimates $b_7^3(1) < 1.6 \times 10^{38}$, and $b_8^3(1) < 9.4 \times 10^{50}$.

7.2 Some upper bounds – Hooley and Heath-Brown

Mordell proved that $u(n)$ (the number of essentially different expressions for n , defined in section 1.1) was not $O(1)$, and Mahler showed it was greater than $(\ln n)^{1/4}$ for infinitely many n . Guy [8] claims that no non-trivial upper bound for $u(n)$ is known.

Silverman [20] provides a fairly quick proof of a stronger version of Mahler’s result (with exponent $\frac{1}{3}$) using the theory of heights, and uses this to deduce that

$$u(n) = \Omega(\log n)^{r/(r+2)}$$

where r is the maximum known rank of $x^3 + y^3 = A$; this leads to

$$\log n_k^3(1) = o(k^{r+2/r}).$$

He claimed $r = 3$ with $A = 657$ using Stephens’ [22] table of elliptic curves, but I suspect $r = 5$ is possible using one of my five-point curves – Silverman’s paper was written before the discovery of even the four-point one.

I tried using Knapp’s form of the conjecture in section 4.2 to compute the ranks of the curves corresponding to $b_5^3(1)$ and $b_5^3(2)$, with the unhelpful results mentioned in that section; I suspect a better approach would be to try to show that the integer points we have are independent, but I could find no information on how to do this.

Given the extremely difficult conjecture that $x^3 + y^3 = K$ can have arbitrarily large rank for suitable K , we would get a bound of the form $\log n_k^3(1) = O(k)$.

It is rather more difficult to work with p_k^3 ; the elliptic curve arguments all provide rational solutions such that you can remove the common denominator to get an integer one, and this is of course useless for finding solutions without common factors. Silverman [19] proved there is some global constant c such that, if $r(n)$ is the rank of $x^3 + y^3 = n$, there are $< c^{r(n)}$ ways of writing $n = a^3 + b^3$ with $(a, b) = 1$; I've found lots of n with three such expressions, but none with four for $n < 2^{60}$.

The literature tends to refer to $\nu(x) = \sum_{i=1}^x (u(i) > 1)$. Hooley [12] showed in 1963 that $\nu(x) = O(x^{2/3} \log \log x \log x^{-1/2})$ using sieve methods, and in 1980 [11] that $\nu(x) = O(x^{5/9+\epsilon})$. Wooley [24] was able in 1995 to derive the same result using only the theory of quadratic forms; again, there is a good exposition in Nathanson [16].

In 1997, Heath-Brown [9] proved that, given any non-singular cubic form $F(w, x, y, z)$ whose solution surface contained three coplanar rational lines, the number of points $N^{(0)}(P)$ with $F(w, x, y, z) = 0$, $w^2 + x^2 + y^2 + z^2 < P^2$, and (w, x, y, z) not lying on one of the rational lines, is $o(P^{4/3+\epsilon})$ for any $\epsilon > 0$, and hence that $\nu(x) = o(x^{4/9+\epsilon})$ for any such ϵ . This is in very good accordance with the numerical results, which suggest an exponent of about 0.45 and which have $N_2^3(x) = kx^{4/9}$ for $k \in (5, 7)$ for all $x \in (2^{28}, 2^{60})$.

Manin conjectures that $N^{(0)}(P) = o(P^{1+\epsilon})$ for all ϵ , which would lead to $N_2^3(x) = o(x^{1/3+\epsilon})$; this also accords with the rather more speculative numerical results where we divided out by powers of $\log x$.

Hooley was able to deduce a lower bound $N_2^3(x) > Ax^{1/3} \log x$ in his 1980 paper [11] by using Ramanujan's original quadratic-form parameterisation; essentially, he finds a region of values for x and y where all four terms are positive, estimates its size, and appeals rather unhelpfully to the results on quadratic forms in Erdős and Mahler [6] to show that the values are not too much duplicated. The $\log x$ factor comes from considering all possible multiples of the smallest solution, and is a partial sum of a harmonic series.

8 Previous work on the fourth-power case

In some ways, this equation is nicer than $x^3 + y^3 = z^3 + t^3$ since solutions in integers are invariably solutions in *positive* integers. However, there is nothing like so wide a theory as the one for elliptic curves available.

8.1 Euler's parameterisation

Hardy and Wright [10] derive the parameterisation below, which was due to Euler, by putting $x = aw + c$, $y = bw - d$, $z = aw + d$, $t = bw + c$. Expanding $x^4 + y^4 - z^4 - t^4$, we get

$$4c(a^3 - b^3) - d(a^3 + b^3) - w^3 + 6(a^2 - b^2)(c^2 - d^2)w^2 - 4a(d^3 - c^3) + b(c^3 + d^3) - w = 0$$

We then insist that $c = a^3 + b^3$ and $d = a^3 - b^3$ to kill the cubic term, divide through by w and solve the linear equation to get

$$w = \frac{3(a^2 - b^2)(c^2 - d^2)}{2(ad^3 - ac^3 + bc^3 + bd^3)},$$

then substitute back in to get

$$\begin{aligned} x &= a(a^6 + a^4b^2 - 2a^2b^4 + 3ab^5 + b^6) \\ y &= b(a^6 - 3a^5b - 2a^4b^2 + a^2b^4 + b^6) \\ z &= a(a^6 + a^4b^2 - 2a^2b^4 - 3ab^5 + b^6) \\ t &= b(a^6 + 3a^5b - 2a^4b^2 + a^2b^4 + b^6) \end{aligned}$$

Here, x and y are 7th-order homogenous polynomials, so $N = x^4 + y^4$ is a homogenous polynomial of degree 28 in two unknowns (in fact, it's of degree 14 in a^2, b^2); we expect this construction with integer parameters to give us $O(N^{1/14})$ solutions less than N , even if we assume all its values are distinct, so it cannot explain all the solutions we see.

8.2 Notes on the results of the exhaustive search, and Zajta's paper

The only article I've been able to find on this problem is Zajta's review article [25] of 1983, which surveys a large number of parameterisation techniques and ends with 218 primitive solutions, derived by all the methods named, with $0 < a, b, c, d < 10^6$; my exhaustive search gave 516 solutions in that range, and 526 with $0 < a^4 + b^4 < 2^{80}$, suggesting that a new idea might be needed to provide a more complete parameterisation.

Unlike in the sixth-power case, we never have $a^4 + b^4 = c^4 + d^4$ with $a^2 + b^2 = c^2 + d^2$, nor do we see any other interesting linear relations between the squares of a, b, c, d . $B_2^4(x)$ does not appear to be of the logarithmic form predicted by the elementary heuristics, but even if we assume that it is $O(x^{1/8})$ (as appears from the graphs) the same heuristics would suggest that $B_3^4(x) \approx x^{1/8}x^{-1/2}$ (the second factor being the probability of a number chosen at random being the sum of two fourth powers), which is too small to hold out hope.

Zajta's most effective technique was the Method of Pythagorean Triples. We begin by pointing out that, given $a^4 + b^4 = c^4 + d^4$, we can write $a = p - q, b = r + s, c = p + q, d = r - s$ and expand to get the equivalent form $pq(p^2 + q^2) = rs(r^2 + s^2)$.

Now, we use the standard parameterisation of Pythagorean triples $a = 2uv, b = u^2 - v^2, c = u^2 + v^2$ with $a^2 + b^2 = c^2$, and take two triples (a_1, b_1, c_1) and (a_2, b_2, c_2) derived from parameters (u_1, v_1) and (u_2, v_2) respectively. We search by some method until we find a pair where $C^2 = A^2 + B^2$ is a perfect square (where $A = a_1c_1 + a_2c_2, B = b_1c_1 + b_2c_2$).

Now A, B, C is also a Pythagorean triple; remove common factors, and solve for the parameters (U, V) generating it. Zajta claims that

$$p = Uu_1 + Vv_1, q = Uv_1 - Vu_1, r = Uu_2 + Vv_2, s = Vu_2 - Uv_2$$

are a valid set p, q, r, s for the alternate parameterization above, and generates a large number of solutions (the difficulty being mostly in checking that C^2 defined as above is actually a perfect square).

9 Possible further work

As computers become faster, and in particular as large memories start appearing at consumer-level prices, it will be possible to take many of these searches significantly further.

For a p much greater than 2^{20} the array of triples in section 3 will not easily fit into memory, and the slicing technique from section 6.1 will have to be used, to reduce the memory requirement in return for a decrease in speed by the same factor. Nonetheless, I expect a search up to $p = 2^{24}$ to be practical with a few months of runtime on a few dozen modern computers.

The search for $\sum_{i=1}^5 x_i^5 = 0$ by my two-list technique does not run into memory limitations as quickly as any of the others, since it is $O(p)$ in memory and $O(p^3)$ in time, so our choice of p is determined by available time. $p = 32779$ was probably about as large as could be handled by handing out work manually.

There are well-known automated techniques for managing distributed computations; $p \approx 2^{19}$ would require similar effort to the successful distributed cryptography problems, and I'd expect at least one more primitive solution to appear in that range.

An interesting goal would be the discovery of a sum $\sum_{i=1}^7 x_i^7 = 0$; my techniques would be able to handle this (if there are three negative and four positive terms) with $O(p^2)$ memory and $O(p^4)$ CPU time, which is just about practical nowadays for $p \approx 2000$. Bob Scher intends to perform such a search in the fairly near future using some interesting extensions of his result for fifth powers.

Whilst there exist faster algorithms for finding $N_C(p)$ than the $O(p)$ method I used – Cohen [1] presents an $O(p^{1/4})$ one – I doubt that it will ever be practical to compute the terms in Knapp's version of the Birch–Swinnerton-Dyer Conjecture up to large enough R to have the curve stable enough to fit a straight line and get a believable estimate of the rank.

References

- [1] H. Cohen, *A course in computational algebraic number theory* (Springer-Verlag, Berlin 1993)
- [2] V. A. Demjanenko, L. Euler's Conjecture, *Acta Arith.* 25 (1973-4) 127-135

- [3] L. E. Dickson, *History of the Theory of Numbers*, (Carnegie Institute, Washington 1919 - 1923)
- [4] R. L. Ekl, Equal sums of four seventh powers, *Math. Comp.* 65 (1996) 1755-1756
- [5] N. Elkies, On $A^4 + B^4 + C^4 = D^4$, *Math. Comp.* 51 (1988) 825-835
- [6] P. Erdős and K. Mahler, On the number of integers which can be represented by a binary form, *J. London Math. Soc.* 13 (1938) 134-139
- [7] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics* (Addison Wesley, Reading MA 1994)
- [8] R. K. Guy, *Unsolved problems in number theory* (Springer-Verlag, Berlin 1994)
- [9] D. R. Heath-Brown, The density of rational points on cubic surfaces, *Acta Arith.* 79.1 (1997) 17-30
- [10] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers, 5th edition* (Oxford University Press, Oxford 1979)
- [11] C. Hooley, On the numbers that are representable as the sum of two cubes, *J. Reine Angew. Math.* 314 (1980) 146-173
- [12] C. Hooley, On the representation of a number as a sum of two cubes, *Math. Z.* 82 (1963) 259-266
- [13] A. W. Knap, *Elliptic curves* (Princeton University Press, Princeton 1992)
- [14] L. J. Lander & T. R. Parkin, Counterexample to Euler's conjecture on sums of like powers, *Bull. Amer. Math. Soc.* 72 (1966) 1079
- [15] J. Leech, Some solutions of Diophantine equations, *Proc. Camb. Phil. Soc.* 1953 778-780
- [16] M. B. Nathanson, *Additive number theory – the classical bases* (Springer-Verlag, Berlin 1996)
- [17] E. Rosenstiel, J. A. Dardis and C. R. Rosenstiel, The four least solutions in distinct positive integers of the Diophantine equation $s = x^3 + y^3 = z^3 + w^3 = u^3 + v^3 = m^3 + n^3$, *Bull. Inst. Math. Appl.* 27 (1991)
- [18] R. Scher, manuscript, 1995
- [19] J. H. Silverman, Integer points and the rank of Thue elliptic curves, *Invent. Math.* 66 (1982) 395-404
- [20] J. H. Silverman, Integer points on curves of genus 1, *J London Math. Soc.* 28 (1983) 1-7

- [21] J. H. Silverman and J. Tate, *Rational points on elliptic curves* (Springer-Verlag, Berlin 1992)
- [22] N. Stephens, The Diophantine equation $x^3 + y^3 = Dz^3$ and the conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* 231 (1968) 121-162
- [23] R. Taylor and A. Wiles, *Ann. of math.* 141, no. 3 (1995)
- [24] T. D. Wooley, Sums of two cubes, *IMRN* 1995 no. 4
- [25] A. J. Zajta, Solutions of the Diophantine Equation $A^4 + B^4 = C^4 + D^4$, *Math. Comp.* 41 (1983) 635-659

A Numbers writable in five ways as a sum of the cubes of two positive integers

$$\begin{aligned}
 48988659276962496 &= 231518^3 + 331954^3 \\
 &= 221424^3 + 336588^3 \\
 &= 205292^3 + 342952^3 \\
 &= 107839^3 + 362753^3 \\
 &= 38787^3 + 365757^3
 \end{aligned}$$

$$\begin{aligned}
 490593442681271000 &= 579240^3 + 666630^3 \\
 &= 543145^3 + 691295^3 \\
 &= 285120^3 + 776070^3 \\
 &= 233775^3 + 781785^3 \\
 &= 48369^3 + 788631^3
 \end{aligned}$$

Reduced to rational form, we get

$$\begin{aligned}
 2636^3 + 4007^3 &= \frac{16537^3 + 23711^3}{6^3} \\
 &= \frac{51323^3 + 85738^3}{21^3} \\
 &= \frac{107839^3 + 362753^3}{84^3} \\
 &= \frac{1847^3 + 17417^3}{4^3}
 \end{aligned}$$

and

$$\begin{aligned}
28512^3 + 77607^3 &= 57924^3 + 66663^3 \\
&= \frac{108629^3 + 138259^3}{2^3} \\
&= \frac{46755^3 + 156357^3}{2^3} \\
&= \frac{48369^3 + 778631^3}{10^3}
\end{aligned}$$

B Ramanujan-style solutions

B.1 General case, $|a|, |b|, |c| \leq 20$

As in the text, let $f_{a,b,c} = ax^2 + bxy + cy^2$. Then

$f_{1,11,9}^3$	+	$f_{-9,-11,-1}^3$	=	$f_{10,20,12}^3$	+	$f_{-12,-20,-10}^3$
$f_{1,9,-1}^3$	+	$f_{2,0,10}^3$	=	$f_{1,-7,-9}^3$	+	$f_{2,4,12}^3$
$f_{2,4,12}^3$	+	$f_{1,11,9}^3$	=	$f_{1,-5,-15}^3$	+	$f_{2,8,18}^3$
$f_{3,1,-7}^3$	+	$f_{-6,-16,-14}^3$	=	$f_{3,17,17}^3$	+	$f_{-6,-20,-20}^3$
$f_{3,1,-7}^3$	+	$f_{5,15,7}^3$	=	$f_{-4,-12,-14}^3$	+	$f_{6,16,14}^3$
$f_{3,5,-5}^3$	+	$f_{-6,4,-4}^3$	=	$f_{-6,8,-6}^3$	+	$f_{3,-11,3}^3$
$f_{3,5,-5}^3$	+	$f_{5,-5,-3}^3$	=	$f_{-4,4,-6}^3$	+	$f_{6,-4,4}^3$
$f_{5,15,7}^3$	+	$f_{4,12,14}^3$	=	$f_{-3,-17,-17}^3$	+	$f_{6,20,20}^3$
$f_{6,3,9}^3$	+	$f_{-5,-9,12}^3$	=	$f_{4,-9,-15}^3$	+	$f_{3,3,18}^3$
$f_{6,3,9}^3$	+	$f_{10,1,-8}^3$	=	$f_{12,9,6}^3$	+	$f_{-8,-17,1}^3$
$f_{6,3,9}^3$	+	$f_{8,17,-1}^3$	=	$f_{9,15,12}^3$	+	$f_{-1,-19,-10}^3$
$f_{6,4,14}^3$	+	$f_{-3,-16,7}^3$	=	$f_{5,0,-17}^3$	+	$f_{4,0,20}^3$
$f_{6,4,14}^3$	+	$f_{-6,4,-14}^3$	=	$f_{3,16,-7}^3$	+	$f_{-3,16,7}^3$
$f_{6,9,12}^3$	+	$f_{-5,-1,16}^3$	=	$f_{4,17,-2}^3$	+	$f_{3,3,18}^3$
$f_{7,17,-17}^3$	+	$f_{17,-17,-7}^3$	=	$f_{-14,20,-20}^3$	+	$f_{20,-20,14}^3$
$f_{8,0,10}^3$	+	$f_{-8,8,-12}^3$	=	$f_{4,14,-9}^3$	+	$f_{-4,18,1}^3$
$f_{8,1,-10}^3$	+	$f_{6,-9,12}^3$	=	$f_{12,-15,9}^3$	+	$f_{-10,19,-1}^3$
$f_{8,3,-14}^3$	+	$f_{6,-17,-7}^3$	=	$f_{12,-5,17}^3$	+	$f_{-10,3,-20}^3$
$f_{9,4,-9}^3$	+	$f_{-12,-16,-12}^3$	=	$f_{1,20,15}^3$	+	$f_{-10,-20,-18}^3$
$f_{9,5,-12}^3$	+	$f_{12,-19,-2}^3$	=	$f_{-15,17,-18}^3$	+	$f_{18,-19,16}^3$

B.2 abb special case, $|a|, |b| < 1200$

Let

$$u_{a,b} = (ax^2 + bxy + by^2)^3 - (bx^2 + bxy + ay^2)^3.$$

We have

$u_{105,33}$	$=$	$u_{70,-92}$	$u_{1092,217}$	$=$	$u_{780,-935}$
$u_{111,-465}$	$=$	$u_{-148,-472}$	$u_{114,-229}$	$=$	$u_{-798,-805}$
$u_{124,-251}$	$=$	$u_{-620,-635}$	$u_{21,-43}$	$=$	$u_{-84,-88}$
$u_{234,-452}$	$=$	$u_{819,763}$	$u_{26,-55}$	$=$	$u_{-78,-87}$
$u_{266,-484}$	$=$	$u_{665,545}$	$u_{28,-53}$	$=$	$u_{84,75}$
$u_{294,-831}$	$=$	$u_{-490,-895}$	$u_{3,-5}$	$=$	$u_{6,4}$
$u_{315,-5}$	$=$	$u_{252,-248}$	$u_{364,40}$	$=$	$u_{273,-303}$
$u_{372,-1000}$	$=$	$u_{-651,-1099}$	$u_{38,-124}$	$=$	$u_{-57,-129}$
$u_{42,-83}$	$=$	$u_{210,205}$	$u_{456,-669}$	$=$	$u_{760,355}$
$u_{65,-127}$	$=$	$u_{260,248}$	$u_{7,-17}$	$=$	$u_{-14,-20}$
$u_{78,-172}$	$=$	$u_{-195,-235}$			

B.3 abc special case, $|a|, |b|, |c| < 256$

As in the text, let

$$w_{a,b,c}(x, y) = (ax^2 + bxy + cy^2)^3 - (cx^2 + bxy + ay^2)^3.$$

Then we have

$w_{3,5,-5}$	$=$	$w_{-4,4,-6}$	$w_{1,11,9}$	$=$	$w_{10,20,12}$
$w_{7,17,-17}$	$=$	$w_{-14,20,-20}$	$w_{18,4,28}$	$=$	$w_{-19,23,21}$
$w_{3,41,-37}$	$=$	$w_{-36,68,-46}$	$w_{30,20,46}$	$=$	$w_{-27,38,37}$
$w_{31,37,-33}$	$=$	$w_{-72,8,-76}$	$w_{21,43,-43}$	$=$	$w_{-84,88,-88}$
$w_{15,50,-49}$	$=$	$w_{-42,68,-58}$	$w_{38,47,-43}$	$=$	$w_{-66,15,-75}$
$w_{13,53,-51}$	$=$	$w_{-104,152,-108}$	$w_{28,53,-53}$	$=$	$w_{-75,75,-84}$
$w_{9,59,-55}$	$=$	$w_{-116,184,-120}$	$w_{-26,55,55}$	$=$	$w_{78,87,87}$
$w_{7,62,-57}$	$=$	$w_{-54,100,-70}$	$w_{19,71,-69}$	$=$	$w_{-60,100,-82}$
$w_{58,20,90}$	$=$	$w_{-59,74,69}$	$w_{23,89,63}$	$=$	$w_{84,172,94}$
$w_{5,85,-76}$	$=$	$w_{-123,213,-132}$	$w_{57,73,-68}$	$=$	$w_{-180,55,-185}$
$w_{33,33,105}$	$=$	$w_{-70,92,92}$	$w_{35,95,59}$	$=$	$w_{92,188,98}$
$w_{42,83,-83}$	$=$	$w_{-205,205,-210}$	$w_{2,97,83}$	$=$	$w_{141,255,150}$
$w_{-15,95,89}$	$=$	$w_{82,148,108}$	$w_{23,101,-97}$	$=$	$w_{-86,148,-116}$
$w_{19,107,-101}$	$=$	$w_{-92,164,-122}$	$w_{23,110,-105}$	$=$	$w_{-94,164,-126}$
$w_{23,125,95}$	$=$	$w_{116,236,134}$	$w_{86,4,134}$	$=$	$w_{-95,110,97}$
$w_{118,116,-44}$	$=$	$w_{123,111,51}$	$w_{85,113,-107}$	$=$	$w_{-220,88,-232}$
$w_{-38,124,124}$	$=$	$w_{57,129,129}$	$w_{-22,148,140}$	$=$	$w_{75,177,147}$
$w_{103,145,-140}$	$=$	$w_{-204,111,-231}$	$w_{-108,148,142}$	$=$	$w_{165,85,205}$
$w_{122,68,188}$	$=$	$w_{-115,155,149}$	$w_{-78,172,172}$	$=$	$w_{195,235,235}$
$w_{85,170,-171}$	$=$	$w_{-138,172,-202}$	$w_{140,20,218}$	$=$	$w_{-151,179,161}$
$w_{164,68,254}$	$=$	$w_{-163,209,197}$	$w_{113,206,-207}$	$=$	$w_{-166,188,-246}$

C Graphs